Departamento de Matemática da Universidade de Coimbra **Álgebra Comutativa**

*SOLUÇÕES* **Frequência** 21/12/2012

---

**1. (a)** $\langle 3\rangle + \langle 4\rangle = \{0,3\} + \{0,2,4\} = \{0,2,4,3,5,1\} = \mathbb{Z}_6$.

**(b)** $\langle 3\rangle \oplus \langle 4\rangle = \{0,3\} \oplus \{0,2,4\} = \{0,3\} \times \{0,2,4\} = \{(0,0),(0,2),(0,4),(3,0),(3,2),(3,4)\}$.

Resolução alternativa: Como $\langle 3\rangle \cap \langle 4\rangle = \{0\}$, então $\langle 3\rangle \oplus \langle 4\rangle \simeq \langle 3\rangle + \langle 4\rangle = \mathbb{Z}_6$.

**(c)** Usando o algoritmo de Euclides, $3+i = 2\times 1 + (1+i)$ e $2 = (1+i)(1-i)+0$, pelo que $\mathrm{mdc}(2, 3+i)$ é o conjunto dos associados de $1+i$, isto é,

$$\mathrm{mdc}(2,3+i)\{1+i, -1-i, -1+i, 1-i\}.$$

Resolução alternativa: Basta observar que as factorizações em irredutíveis de 2 e $3+i$ são $2 = (1+i)(1-i)$ e $3+i = (1+i)(2-i)$.

**(d)** Basta olhar para $x^3 + x^2y + xy^2 + y$ em $\mathbb{K}[y][x]$ e observar que $y$ é um elemento irredutível de $\mathbb{K}[y]$ que está nas condições do critério de Eisenstein (Prop. 3.9, Cap. 1): $y$ divide $y$ e $y^2$ mas $y \nmid 1$ e $y^2 \nmid y$.

**(e)** Temos

$$\begin{aligned}\mathbb{Z}_{20} \oplus \mathbb{Z}_{40} \oplus \mathbb{Z}_{108} &= \frac{\mathbb{Z}}{\langle 2^2 \times 5\rangle} \oplus \frac{\mathbb{Z}}{\langle 2^3 \times 5\rangle} \oplus \frac{\mathbb{Z}}{\langle 2^2 \times 3^3\rangle} \\ &\simeq \frac{\mathbb{Z}}{\langle 2^2\rangle} \oplus \frac{\mathbb{Z}}{\langle 5\rangle} \oplus \frac{\mathbb{Z}}{\langle 2^3\rangle} \oplus \frac{\mathbb{Z}}{\langle 5\rangle} \oplus \frac{\mathbb{Z}}{\langle 2^2\rangle} \oplus \frac{\mathbb{Z}}{\langle 3^3\rangle} \\ &\simeq \mathbb{Z}_4 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{27}.\end{aligned}$$

Esta última é a decomposição em factores cíclicos primários. Os respectivos divisores elementares são então as potências primas $2^2, 5, 2^3, 5, 2^2, 3^3$. Consequentemente, os factores invariantes são

$$\begin{array}{ccccccccc} 2^2 & \times & 3^0 & \times & 5^0 & = & 4 \\ 2^2 & \times & 3^0 & \times & 5 & = & 20 \\ 2^3 & \times & 3^3 & \times & 5 & = & 1080 \end{array}$$

e a decomposição em factores cíclicos invariantes é $\mathbb{Z}_4 \oplus \mathbb{Z}_{20} \oplus \mathbb{Z}_{1080}$.

**2. (a)** A unicidade de $\overline{f}$ é evidente, uma vez que a comutatividade do diagrama obriga a que, para cada $v + N_1 \in M_1/N_1$,

$$\overline{f}(v+N_1) = \overline{f}(\pi_1(v)) = \pi_2(f(v)) = f(v) + N_2. \qquad (*)$$

Bastará agora verificar que esta condição define de facto um homomorfismo de $A$-módulos, o que é simples:

- Uma vez que $f$ é um homomorfismo e $f(N_1) \subseteq N_2$, então $v + N_1 = w + N_1 \Leftrightarrow v - w \in N_1 \Rightarrow f(v) - f(w) = f(v-w) \in N_2 \Leftrightarrow f(v) + N_2 = f(w) + N_2$ (o que assegura que $(*)$ define uma aplicação em $M_1/N_1$).

- $\overline{f}((v+N_1)+(w+N_1)) = \overline{f}(v+w+N_1) = f(v+w)+N_2 = f(v)+f(w)+N_2 = (f(v)+N_2)+(f(w)+N_2) = \overline{f}(v+N_1)+\overline{f}(w+N_1)$.
- $\overline{f}(a(v+N_1)) = \overline{f}(av+N_1) = f(av)+N_2 = af(v)+N_2 = a(f(v)+N_2) = a\overline{f}(v+N_1)$.

**(b)** $\Rightarrow$: Suponhamos que $\overline{f}$ é bijectiva. Então:

- Se $v \in f^{-1}(N_2)$ então $f(v) \in N_2$, logo $f(v)+N_2 = 0$, isto é, $\overline{f}(v+N_1) = 0$. Como $\overline{f}$ é injectiva, então $v+N_1 = 0$, isto é, $v \in N_1$.
- Seja $w \in M_2$. Então $w+N_2 \in M_2/N_2$ e, pela sobrejectividade de $\overline{f}$, existe $v \in M_1$ tal que $\overline{f}(v+N_1) = w+N_2$. Mas então $f(v)+N_2 = w+N_2$, ou seja, $w-f(v) \in N_2$. Portanto, $w = f(v)+(w-f(v)) \in \mathrm{Im}(f)+N_2$.

$\Leftarrow$:

- $\overline{f}$ é injectiva: Se $\overline{f}(v+N_1) = \overline{f}(w+N_1)$ então $f(v)-f(w) \in N_2$, isto é, $f(v-w) \in N_2$. Portanto, $v-w \in f^{-1}(N_2) \subseteq N_1$. Logo $v+N_1 = w+N_1$.
- $\overline{f}$ é sobrejectiva: consideremos um elemento $w+N_2$ de $M_2/N_2$. Por hipótese, existem $v \in M_1$ e $w' \in N_2$ tais que $w = f(v)+w'$. Mas então $w+N_2 = f(v)+N_2 = \overline{f}(v+N_2)$.

**3. (a)** Como vimos, qualquer anel comutativo com identidade $A$ é um $A$-módulo (onde as duas operações de módulo são dadas pelas duas operações do anel). Os submódulos do $A$-módulo $A$ são os ideais de $A$: $S \subseteq A$ é um submódulo de $A$ se e só se $S \neq \emptyset$ e $a_1s_1 + a_2s_2 \in S$ para quaisquer $a_1, a_2 \in A$ e $S_1, s_2 \in S$. Isto significa que $S$ é um subgrupo de $(A,+)$ tal que $as \in S$ para quaisquer $a \in A$ e $s \in S$, ou seja, que $S$ é um ideal do anel $A$. Portanto, *os submódulos do $A$-módulo $A$ são precisamente os ideais do anel $A$.*

No caso $A = \mathbb{Q}$, como se trata de um corpo, os únicos ideais de $\mathbb{Q}$ são os triviais: $\{0\}$ e $\mathbb{Q}$ (de facto, se $q \neq 0 \in S$ então $1 = q^{-1}q \in S$; daí decorre imediatamente que $S = \mathbb{Q}$). Logo, estes são os únicos submódulos.

**(b)** É óbvio que $\{1\}$ é uma base de $\mathbb{Q}$ (como $\mathbb{Q}$-módulo). Como $\mathbb{Q}$ é um corpo, possui a propriedade da invariância dimensional, pelo que $\dim \mathbb{Q} = 1$.

**(c)** Suponhamos que
$$\frac{a_1}{b_1}, \frac{a_2}{b_2}, \ldots, \frac{a_k}{b_k}$$
era um conjunto de geradores do $\mathbb{Z}$-módulo $\mathbb{Q}$ (ou seja, do grupo abeliano $(\mathbb{Q},+)$). Estes elementos só conseguem gerar racionais da forma
$$n_1\frac{a_1}{b_1} + n_2\frac{a_2}{b_2} + \cdots + n_k\frac{a_k}{b_k} \quad (n_1, n_2, \ldots, n_k \in \mathbb{Z}),$$
ou seja,
$$\frac{n_1a_1b_2\ldots b_k + n_2a_2b_1b_3\ldots b_k + \cdots + n_ka_kb_1\ldots b_{k-1}}{b_1b_2\ldots b_k}.$$
Assim, qualquer racional que não seja da forma
$$\frac{z}{b_1b_2\ldots b_k}$$

não seria gerado, como por exemplo o racional

$$\frac{1}{2b_1b_2\dots b_k}.$$

**(d)** Seja $I$ um ideal de $D$. Por hipótese (e pela alínea (a)), $I$ é um $D$-módulo livre, ou seja, tem uma base $\mathcal{B}$. Mas qualquer base de $I$ só pode conter um elemento pois quaisquer dois elementos $a, b \in I$ são linearmente dependentes: $(-b)a + ab = 0$. Assim, $\mathcal{B}$ é um conjunto singular, o que mostra que $I$ é principal.

**4. (a)** É fácil verificar que $\mathcal{S}$ é um anel comutativo com identidade!... A sequência $(1, 0, 0, \dots)$ é a identidade.

**(b)** Seja $(a_n)_{n\in\mathbb{N}_0} \in \mathcal{S}$. Suponhamos que $(a_n)_{\mathbb{N}_0}$ é uma unidade de $\mathcal{S}$. Portanto, existe uma sequência $(b_n)_{\mathbb{N}_0}$ tal que $(a_n)(b_n) = 1$. Então $a_0b_0 = 1$ e, consequentemente, $a_0$ é uma unidade de $A$.

Reciprocamente, suponhamos que $a_0 \in A^*$ e consideremos a sequência $(b_n)_{\mathbb{N}_0}$ definida por

$$b_0 = a_0^{-1},\ \ b_1 = -a_0^{-1}(a_1a_0^{-1})\ \ ,\ \dots\ ,\ \ b_k = -a_0^{-1}(a_1b_{k-1} + \cdots + a_kb_0), \quad k \geq 2.$$

É claro que

$$\begin{aligned} a_0b_0 &= 1, \\ a_0b_1 + a_1b_0 &= a_0(-a_0^{-1}(a_1a_0^{-1})) + a_1a_0^{-1} = 0, \\ &\vdots \\ a_kb_0 + a_{k-1}b_1 + \cdots + a_0b_k &= a_kb_0 + a_{k-1}b_1 + \cdots + a_0(-a_0^{-1}(a_1b_{k-1} + \cdots + a_kb_0)) = 0, \end{aligned}$$

pelo que $(a_n)(b_n) = 1$.

**(c)** Suponhamos que $A$ é um corpo. Seja $I$ um ideal de $\mathcal{S}$. Se $I = \{0\}$, então $I$ é principal. Suponhamos então que $I \neq \{0\}$ e definamos a *ordem* de uma sequência $(a_n)$ não nula de $\mathcal{S}$ como sendo o primeiro inteiro não negativo $n$ tal que $a_n \neq 0$ (portanto, $a_n \neq 0$ e $a_i = 0$ para qualquer $i < n$). Claro que existe uma sequência $(a_n)$ em $I$ cuja ordem, digamos $k$, é $\leq$ que a ordem de qualquer $(b_n)$ em $I$. Seja $(c_n)$ a sequência definida por $c_i = a_{k+i}$ para cada $i \geq 0$. Uma vez que $A$ é um corpo, podemos concluir pela alínea anterior que existe $(c_n)^{-1}$ e

$$(c_n)^{-1}(a_n) = (d_n) \in I.$$

Além disso, $d_k = 1$ e $d_i = 0$ para $i \neq k$. Provemos que $I = \langle (d_n) \rangle$:

A inclusão $\langle (d_n) \rangle \subseteq I$ é evidente. Consideremos $(b_n) \in I$, de ordem $m$. Então $m \geq k$. Seja $(r_n)$ o elemento de $\mathcal{S}$ definido por

$$r_{m-k+i} = b_{m+i} \text{ para } i \geq 0 \quad \text{ e } \quad b_i = 0 \text{ para } i \leq m-k.$$

É fácil verificar que $(b_n) = (r_n)(d_n) \in \langle (d_n) \rangle$.